Towards a Multidisciplinary Framework to Include Privacy in the Design of Video Surveillance Systems

Zhendong Ma[1], Denis Butin[2], Francisco Jaime[3], Fanny Coudert[4], Antonio Kung[5], Claire Gayrel[6], Antonio Maña[3], Christophe Jouvray[5], Nathalie Trussart[6], Nathalie Grandjean[6], Víctor Manuel Hidalgo[7], Mathias Bossuet[8], Fernando Casado[3], and M. Carmen Hidalgo[3]

[1] Austrian Institute of Technology
[2] Inria, Université de Lyon
[3] Universidad de Málaga
[4] KU Leuven - Interdisciplinary Centre for Law & ICT - iMinds
[5] TRIALOG
[6] Université de Namur
[7] Visual Tools
[8] THALES

Abstract. Privacy impacts of video surveillance systems are a major concern. This paper presents our ongoing multidisciplinary approach to integrate privacy concerns in the design of video surveillance systems. The project aims at establishing a reference framework for the collection of privacy concepts and principles, the description of surveillance contexts, surveillance technologies, and accountability capabilities.

Keywords: Video surveillance, privacy, accountability, multidisciplinarity, SALT, PARIS

1 Introduction

Despite contested views on its usefulness [15], video surveillance has been widely deployed to protect individuals and assets in public and private spaces. Over the past decades, video surveillance technologies have made tremendous advances, from analogue closed-circuit television (CCTV) to digital and network-based systems. State of the art video surveillance systems are labelled as "smart" and "intelligent", in which different types of information systems are integrated for correlating information from multiple sources. For example, biometric systems can be integrated into video surveillance for individual identification. In addition, advanced video analytic capabilities enable the system to monitor, detect, and search objects and events, e.g., for motion, behaviour, and abandoned object detection. As the systems are often network-based, real-time video streams and recorded video data can be distributed or remotely accessed using existing network infrastructure across geographic and organizational boundaries.

Privacy has always been a concern in surveillance systems. A large amount of work has been carried out in the past, e.g., from political science [21] to technological solutions [17]. However, the rapid development of technologies and the increasing market demand for surveillance capabilities outpace the development of regulations, social norm, and protection mechanisms. As a result, many areas remain partially or entirely undefined, which poses serious privacy risks if they are not handled correctly during the system planning, design, and development phases.

Video surveillance systems can be deployed in disparate contexts and often integrate subcomponents such as access control, communications, and mission management systems. Usually the system design process is driven by operational missions and generic specifications, in which system designers fulfill the technical and operational specifications. During the design process, many options exist and numerous decisions must be taken. This makes it demanding to include and address privacy concerns in the design. For example, perceptions of privacy vary according to context. Notably, expectations in public spaces are usually different from expectations in private ones; yet the demarcation between public and private spaces is sometimes blurry. Accordingly, social, political, and ethical approaches are required to deal with the complexities of those varying perceptions. Furthermore, just within Europe, regulations differ considerably even across member states. Even when only a given country is under consideration, it often remains difficult to find synthetic information about statutory law or case law related to specific surveillance scenarios. A parallel challenge is how to make all the privacy solutions practical, i.e., we must find optimal solutions for individuals' right to privacy on one side and the public need for safety and (homeland) security on the other side.

This paper presents our ongoing work on the establishment of a multidisciplinary framework that includes privacy concerns in the design of video surveillance systems. Specifically, the framework serves as a foundation for the collection of concepts and principles and for the description of surveillance context as well as surveillance technologies and accountability capabilities. It takes into account views from different stakeholders such as policy makers, regulators, national Data Protection Authorities, law enforcement, public authorities, and video surveillance system providers and operators. The framework is envisioned to help designers and other stakeholders facing these complexities to create video surveillance systems taking into account privacy requirements in a methodological, principled, systematic, and accountable way. To this aim, the framework provides reusable, generic and synthetic guidelines, reference information and criteria to be used or modified by experts and other stakeholders.

The remainder of the paper is structured as follows. We describe the privacy challenges and motivate the need for a multidisciplinary framework in § 2. We then give an overview of our approach and the rationales in § 3. The framework and its associated processes are presented in § 4 and § 5, respectively, followed by a summary in § 6.

2 Privacy Challenges and Motivations for Developing a Framework

Privacy is multifaceted, subjective, and evolving. The definition and perception of public and private spaces are constantly shaped under social, political, legal, and cultural influences. Therefore, a consistent basis is needed for describing the context concerning the balance between privacy and surveillance. Otherwise, it is difficult to determine the nature of personal and sensitive information in the surveillance context. Even though privacy can be seen from many angles, we base our analysis on the *Seven Types of Privacy* taxonomy [13], a recent framework (published in 2013) broadening the definition of privacy to account for novel threats introduced by technologies such as surveillance systems. This taxonomy enumerates the following categories: the privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association. While we also included more technical perspectives on privacy in our literature review, the above taxonomy provides a comprehensive categorization independently of specific practical measures to counteract privacy threats.

A chief challenge to video surveillance is the tension between surveillance functionality and privacy. Modern computer vision algorithms are capable of transforming and masking regions of video images that are considered private [10]. However, the willingness of surveillance operators to embrace these solutions in their systems and their effectiveness to protect privacy in systems with multiple information sources are still questionable. Besides, the reliability of these privacy protection components in large scale surveillance systems are yet to be proved. Surveillance systems are not much different from other IT systems that have various potential risks. Any data breach resulting from accidental disclosure or from a malicious attack will have an impact on privacy as well. To make the matter more complex, the trend in surveillance systems is towards multi-model and multi-operator system with increasing system interoperability, which leads to higher co-operation and exchange of information at the organizational level as well as at the system level.

Another challenge to privacy is the imbalance of power between citizens and surveillance system owners, introduced by the massive collection of personal data by surveillance system owners in an opaque way. The lack of knowledge about what is recorded and the absence of an individualised relation with controllers put data subjects in an overly weak position. Because of their inherent opacity, surveillance systems cannot rely on informed consent to legitimate personal data processing. Therefore, data subjects can only rely on *ex post* protection, i.e., complaints and redress procedures. Such protection often come too late and is uncertain in its outcome.

Costs can also be a challenge if alterations or extensions required to support privacy in a system are significant and expensive. Adopting a privacy-by-design approach and taking into account such requirements early on in system design can mitigate this issue.

The number of entities generally involved in surveillance systems yield additional difficulties. Numerous interacting entities generate a multitude of communication channels, often carrying sensitive data. This imbalance and complexity motivate the need to increase the accountability obligations of data controllers for their data processing. By accountability [9], we do not merely mean legal compliance but (1) the demonstration and verifiability of compliance at all levels through transparency about policies, actual processing and the explicit definition of technical compliance and (2) the possibility for an independent third party to actually check the evidence of both legal and technical compliance (e.g., procedure documentation and audit logs). A good definition of the spirit of accountability can be found in an Article 29 Working Group's Opinion [6], which affirms in particular accountability's role of "showing how responsibility is exercised and making this verifiable". Rather than a part of privacy, we consider accountability as a principle and a set of tools that can be used to support it.

While it could be argued that the inherent imbalance of power in any surveillance system brings an ethical obligation upon data controllers to act in a transparent way towards data subjects, the upcoming European General Data Protection Regulation [12] introduces a legal obligation to be able to demonstrate compliance with the data protection framework. This obligation goes through the implementation of adequate policies, procedures and technical measures tending to evidence compliance. Therefore, data subjects or their representatives are owed "accounts", but this is not sufficient; this evidence of the actions of controllers must be analysed and the conclusions of legal and technical compliance checking made available. The regulation foresees that assurance is provided through internal or external audit and legal compliance checked by Data Protection Authorities. However, in terms of technical compliance, both the accounts and the obligations against which they are to be verified often remain vague, impeding meaningful analysis and the reaching of clear conclusions. Furthermore, technical compliance checking on the system level, if it is not completed by links to higher-level principles, may seem excessively technical or disconnected from the big picture to stakeholders. A framework with sufficient generality is therefore needed to integrate the technical and high-level aspects of accountability into a unified approach.

2.1 Existing Work on Privacy and Video Surveillance

Existing research work addresses privacy from either social or computer science perspective, or the combination of both. In recent years, the European Commission funded a number of research projects that touch upon privacy and ethics of surveillance systems. The IRISS project [1] looks at the impact of surveillance technologies on basic rights and their social and economic influences. The SAPIENT project [3] aims at developing a Privacy Impact Assessment (PIA) methodology for surveillance technology. The SurPRISE project [4] assesses criteria and factors influencing European citizens' acceptance of surveillance technology. VideoSense [5] works on privacy preserving video analytics.

Existing solutions fostering accountability include PIA [22]. PIA forces data controllers not only to identify the impact the system developed will have on privacy and implement the necessary safeguards, but also to ensure that compliance with the legal framework is ensured throughout the whole lifecycle of the system which means allocating responsibilities for compliance between the different actors and implementing the required procedures to provide regular reviews and assurance.

PIA should integrate accountability as a system design prerequisite to ensure obligations are fulfilled. In particular, accountability over actual data handling practices is important to increase transparency regarding real system activity. This aspect is often neglected in PIA, yet seems essential to take into account accountability requirements. Even though checks related to accountability are not always part of PIA, adequate technical tools already exist. Available means to achieve this accountability of practice include privacy policy languages such as EPAL [7] or PPL [20], which allow the precise specification of (technical) data handling policies. These standardised policies can then be used to analyze system operation traces (audit logs) through a posteriori technical compliance control [8, 11].

Many technical solutions have surfaced addressing the privacy issue along the line of software, hardware, and system architecture. For example, digital signal processors can be embedded in the so-called "smart cameras", which are then programmed to selectively de-identify, mask, or scramble a certain region in the video [10]. The access to the raw video data is limited. Instead, metadata is used to fulfill the requirement of the surveillance operators. Therefore, video data from the smart cameras is split into two streams: a metadata stream for describing objects, events, behaviour, and other situations in the video; and an image stream which is the original video data.

Senior et al. [18] proposed to foster privacy through a layered access model enforced by a multilevel access control system architecture. The access model derives access rights from the following questions: (1) what data is present, (2) has the subject given consent, (3) what form does the data take, (4) who sees the data, (5) how long is data kept, and (6) how raw is the data. The answers to these questions lead to a layered access model. The raw video stream is further processed, and information is extracted to generate versions of different image details. For example, the access model can include three layers for three types of users: ordinary users can only access statistical information, privileged users can access limited individual information, and law enforcement agencies can access raw video information. For privacy protection, video data are rendered to transform a person's image into a bar, a box, or only its silhouette. Commercial systems such as IBM Smart Surveillance Solutions [16] claim to feature video analytics-based privacy protection mechanisms, including the limitation of access to camera and functions, information extraction from videos, and fuzzy metadata representation.

3 The SALT Approach

The previous section shows that systematically addressing privacy in video surveillance systems requires careful considerations from multiple perspectives. To include privacy from the very beginning of a video surveillance project is crucial for ensuring privacy after the system is deployed and operated, until it is decommissioned. Designers are challenged by choices reflecting concerns from various aspects. Therefore, in order to include privacy in the design of video surveillance systems, a methodological approach is required to systematically address multidisciplinary concerns.

We aim at ensuring that the designed system supports both public security interests and minimal impact on individuals' privacy. Accountability mechanisms are further given specific attention to increase transparency and help reinforcing citizen rights in a surveillance society (or faced with surveillance systems). To achieve these goals, a methodology is defined based on a two-step process:

1. System owners[9] are first guided through a reflexive process to assess the legal/socio-contextual[10] and ethical opportunity of the system envisioned, i.e. to assess the necessity and proportionality of the technology in relation to the stated purposes. Assessment of the impact on individuals' privacy as framed under the *Seven Types of Privacy* terminology [13] is a key at that stage. This phase could lead to discard, validate or mitigate the options initially taken.
2. During the design process, designers[11] are referred to socio-contextual, ethical and legal considerations that should be taken into account in order to reduce the impact of the system on individuals' privacy. They are presented with state-of-the-art privacy preserving technologies to mitigate such impact and with accountability features to increase the level of transparency of the system and the traceability of the actions performed by such system.

The outcome of these two stages (opportunity assessment and system requirements) are documented in order to enable legal validation but also to enhance the transparency of the decision-making process.

Two pillars are defined to support the methodology:

– A decision support in the form of a knowledge base to assist the understanding of common concerns in complex and evolving environments and to facilitate the decision-making process. We identify the social-contextual, ethical, legal, and technological aspects as the most influential factors in the decision

[9] In this paper, system owners are defined as a legal entity (for basic systems, this can be a person or a group of persons) that has the ownership of the system (meaning its hardware and software components).

[10] We use the word "contextual" to emphasize the need to take into account local (at the country or regional level) perceptions of privacy and surveillance.

[11] We define system designers as the entities producing sufficient, coherent and testable specifications for a given system.

support, which is referred to as the SALT framework. The SALT framework is envisioned to provide a guidance for system designers to design and integrate privacy and accountability into the system and to enforce high level requirements in technical terms during the product lifecycle. § 4 describes the SALT framework.
– Processes associated with the SALT framework, which specify what knowledge should be included in the SALT framework, and how to use the knowledge to support the design of video surveillance systems that integrate privacy and accountability from the start, i.e., privacy-by-design and accountability-by-design. §. 5 describes the processes in details.

4 SALT Framework

The SALT framework is a collection of concepts and overarching principles concerning privacy including social-contextual, ethical, legal, and technical viewpoints. It is envisioned to be a reference for decision support during the design of video surveillance systems. The present section describes how to collect and synthesize knowledge from various views into the framework, and how to process and manage the knowledge in the framework.

4.1 Overview

The SALT framework relies on the SALT management tool, a set of computer programs that enable a user (a person acting for a surveillance system operator or a domain expert), to interact with concepts and information stored in the computer. The work on knowledge capture and management in the SALT framework is inspired from the principles and methods of knowledge engineering, in which building a knowledge-based system is regarded as a modelling process, i.e., constructing computer models for realizing problem-solving capabilities comparable to the ones of a domain expert [19].

Fig. 1 provides an overview of the SALT framework. It relies on literature and domain experts as knowledge sources. The literature includes academic research articles, legal texts, institutional and policy documents, and studies funded by the European Commission. In addition, a possible extension to the knowledge source can be the opinions of other stakeholders such as citizens and relevant associations and organisations. Initially, the domain experts are mainly the individuals creating the SALT framework. SALT knowledge is selectively captured in a number of ways that are deemed relevant. In this stage, experts' effort will be needed to evaluate the relevance of captured knowledge. Since SALT knowledge comes from different disciplines and individuals, work is also needed to identify links and synthesize knowledge coherently.

The analysed knowledge is transferred from textual description to defined models which facilitate the management of captured knowledge. In other words, models are structured, machine-readable presentations of information related to privacy and video surveillance. The SALT knowledge repository stores these

models from various sources. The purpose of knowledge application is to assist system designers to apply the knowledge to solve similar problems in an efficient and correct way. In other words, given the information on a specific context such as legal system and surveillance project requirements, one can retrieve tailored references for decision support in system design phase. This specific information helps designers to take proper design decisions to develop surveillance systems and to enforce social, ethical, and legal requirements in technical terms such as appropriate access control models and the implementation of audit trails.

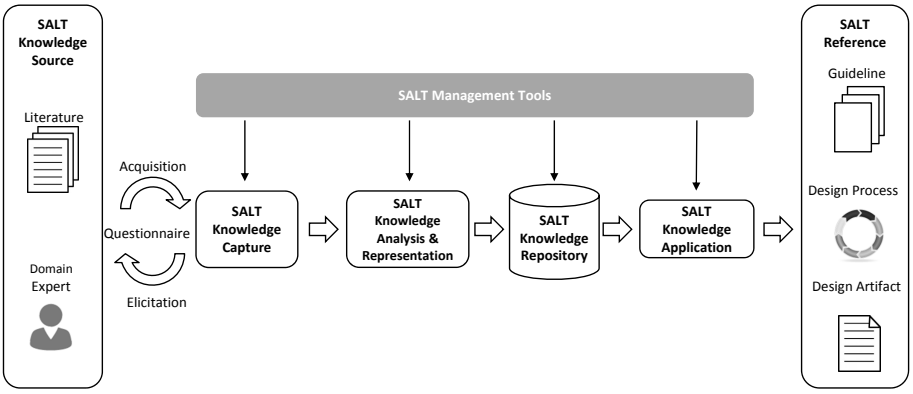

Fig. 1. Knowledge engineering in SALT framework

As a collection of knowledge from various sources, the SALT framework will be accessed and edited by different users in a cooperative way. Thus the role of the SALT management tools is to provide tool support for the creation, edition, search, and extraction of the knowledge in the SALT framework.

The SALT compliant design process is envisioned to ensure the proportionality of the surveillance purpose and of the system designed, by integrating privacy requirements into the design process according to the instantiated SALT framework.

For instance, the aspect of the design process focusing on accountability takes into account a number of aspects at different levels, involving corresponding disciplines. Its overarching goal is to encourage controllers into increased transparency. At the most general level, enabling accountability requires identifying all entities involved in the surveillance infrastructure, which data they have access to and under which conditions. The responsibilities of all actors in terms of protecting privacy and processing personal data in compliance with the data protection framework must also be clarified.

For the controller to be able to account for its policy, policies regulating data users should be transparent to Data Protection Authorities. This involves not only compliance with the legal framework but also the active demonstration of links between the privacy policy and the legal obligations to which they

correspond to. This simplifies subsequent verification of legal policy compliance. In addition, subjects must know what is recorded and which entities can access which recordings under which conditions. For instance, in some surveillance systems, massive amounts of recording channels exist with thousands of cameras deployed in urban areas. Thus multiple control centers are required to handle this kind of data production, making it extremely complex to identify all data flows, access authorizations, purposes of the data processing and ultimately to enforce the internal privacy policy of the organization. In such cases, the importance of accountability, i.e., of the transparency of the data processing operations as well as a proper allocation of responsibilities, is vital to mitigate privacy risks.

At a different but equally important level, appropriate procedures must be implemented. They involve integrating privacy concerns into business processes, carrying out PIA, appointing a Data Protection Officer who is responsible for ensuring internal compliance, training staff and carrying out periodic audits.

Finally, policies and procedures should translate into practice. Technical measures can help data controllers to demonstrate that their practices actually meet the requirements of the legal framework. In SALT compliant design process, this involves taking a closer look at the details of the entire data lifecycle, including the exact nature of recorded data, temporal parameters such as the maximal duration of storage and storage security (which may use cryptography). Because data is recorded in public spaces, there can be no one-on-one data handling policy negotiation between a subject and the controller. Instead, a representative of the public may defend the interests of individual subjects by globally negotiating privacy policies during the SALT complaint design process. Some traditional data protection principles, such as data minimization, may be difficult to apply in some cases, for instance when images are recorded. However, specific techniques, for instance the automatic blurring of faces, may be available to promote this principle. These techniques are a part of the possible design artifacts presented to system designs.

4.2 SALT Knowledge Management

In the initial phase, the knowledge input of the SALT framework mainly relies on systematic literature review and guided interview of domain experts. In the systematic literature review, a team of researchers and engineers from various disciplines has conducted a breadth-first survey of existing body of knowledge on privacy and surveillance. The scope of the survey covers psychosocial, social, political, ethical, legal, and computer engineering topics related to privacy in surveillance systems. Our literature review also includes topics on accountability-by-design, privacy-by-design, and PIA [14].

Another source of knowledge input comes from domain experts or other stakeholders through proactive elicitation. The elicitation process is conducted and guided by questionnaires. The questionnaires are carefully designed to capture knowledge related to specific aspects of the SALT framework. For example, our preliminary questionnaire for eliciting legal knowledge for surveillance systems include questions in three stages: (1) a preliminary assessment of legitimacy and

overall proportionality of surveillance systems in relation to the stated purpose; (2) the assessment of surveillance system following Article 29 Working Party guidance and Directive 95/46 principles; and (3) the assessment of balancing *stricto sensu*. The knowledge is captured in an iterative process, i.e., the analysis of the knowledge acquired will provide additional guidance on how knowledge is elicited by modifying the structure and content of the questionnaire.

The knowledge in the SALT framework must also be accessed and extended to account for the evolving nature of privacy concerns. In order to do so in an efficient and user-friendly way, the knowledge in SALT framework should be machine-readable, i.e. we need to transfer the knowledge into an appropriate computer representation such that a computer is able to work on it. The computer-readable representation of the SALT knowledge can be realised in various ways, depending on the type of technology and platform chosen. Typical examples include XML, JSON, or a Wiki-based structure. However, independently of the representation language and platform, it is important to have a high level definition of the structure and format of the SALT knowledge. From a computer engineering point of view, it is analogous to the definition of models for representing and processing information. In the case of the SALT framework, this model is what we call a *SALT template*. Whenever a piece of knowledge is added to the SALT framework, it follows the structure given by the SALT template, that is, we instantiate the SALT template according to the knowledge and then we store it. We name the result a *SALT instance* or a *SALT reference*[12].

The proposed SALT template must fulfil the following properties: (1) it must allow to differentiate each particular instance, (2) each instance must be uniquely identified, (3) it must prove the reliability of the information that it stores, (4) it must include the key information regarding the privacy or accountability concerns that it handles, and (5) it must provide a mechanism that allows for storing information coming from the four different categories, which may need different ways of handling the information.

In order to achieve these requirements, we have devised the structure depicted in Fig. 2. A SALT template contains several types of components. At the first level, it includes the instance information and the content. *Instance information* is unique to each SALT instance and is used to differentiate instances. An instance includes *Identification*, which identifies the SALT instance, typically an instance identifier or a version number; and *Trust information*, which is used to guarantee SALT information trustfulness. To ensure the integrity and authenticity of the reference information, trust mechanisms such as digital signatures, authority identifiers, certifications or trusted-party endorsements can be included. Another part of a SALT instance is the *Content* component, which stores the information related to the actual concerns. The content includes *Core information*, which identifies what type of concern is stored within the SALT instance, e.g. concern identifiers and concern categories, and *Extensions*, which provides the rationale and information related to a specific concern. For example, *Ethical extension*

[12] In this paper, "SALT reference" and "SALT instance" will be used interchangeably since they refer to the same concept but reflect different disciplinary perspectives.

includes information on topics such as types of privacy likely to be impacted by the surveillance system, stakeholders who need the system, affected individuals' basic rights and so on.

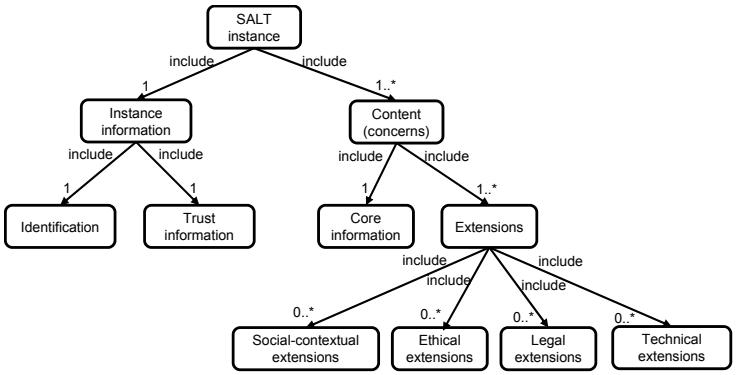

Fig. 2. Structure and components of SALT instance

Each new instance will include the information on the origin of the knowledge and the author(s) of the instance such that the content of the instance can be checked if necessary. Since decisions on privacy-related issues are results of specific contexts, such as the case of different interpretations of the same law, it is possible that there might be overlapping instances. A probable solution is to provide all related instances to system designers to help them to make a decision. Since concerns have different levels of specificity, for example, legal concerns usually depend on specific cases while social concerns can be linked to more general context, the SALT template is designed to be flexible enough to be useful for both specific and general cases.

5 SALT Process

Three independent processes are closely associated with the SALT framework and define how privacy concerns are captured, managed, and applied. The processes can be divided into two groups according to their purposes: SALT knowledge building processes and SALT knowledge use process. With SALT knowledge building processes, we decide what relevant information to take into account and how to integrate it into the SALT framework. For this purpose, two different processes are defined: *Information acquisition process* and *Information representation process*. SALT knowledge use process describes how information gathered by previous processes can be used to guide system designer during the system design phase. In the context of SALT framework, this process is called *SALTed design process*.

5.1 Information Acquisition Process

We define this process to describe how to acquire information for the SALT framework. Depending on the type of concerns (i.e., socio-contextual, ethical, legal and technical), there are different methods to gather the information.

Questionnaires Questionnaires are a convenient method for extracting information regarding socio-contextual and ethical concerns. Due to the nature of these concerns, any meaningful result requires to match the knowledge of a sample group of individuals, which must be big enough in order to be representative of a population. Therefore, questionnaires, and the subsequent analysis of the obtained data, are an appropriate method to achieve this task.

Primary sources This method involves the systematic review of documents and reports for objective information, i.e. information that is less likely to be influenced by personal and subjective feelings and interpretations. Legal and technical concerns in the SALT framework are the ones that clearly benefit from this type of documentation. Numerous legal documents (constitutions, licenses, proclamations, statements, sureties, tax forms, treaties, etc.) and technical reports are widely accepted and trusted. They provide objective information and views to the SALT framework.

Secondary sources Apart from the two previous methods for information acquisition, domain experts can provide valuable input as a direct result of their own expertise in the form of personal opinions and decisions that may apply to ambiguous issues. For example, a lawyer could provide a possible interpretation of a given law applied to a determined context.

5.2 Information Representation Process

As its name states, this process handles the task of representing the information acquired from the information acquisition process. The information is modeled and stored in the knowledge repository. Therefore, the structure and format of a SALT instance is crucial, since they directly affect to the performance of the knowledge management. The modeling of a SALT instance is covered in §. 4.2.

5.3 SALTed Design Process

The SALTed design process designates the SALT reference usage process that will guide system designers in the design of a SALT compliant surveillance system. SALT compliance signifies that the system design process includes relevant privacy concerns and follows the guidelines specified by the SALT framework. It starts from the SALT instances selection and ends with the creation of a system design specification. The SALTed design process is designed in a way that makes it

likely to be adopted by system designers (usually engineers or other technical staff) while minimizing interference with existing system design processes and workflows. Besides, in order to assess the reliability of the content provided by these experts, an evaluation mechanism might be created in the future to decide their level of expertise.

Tab. 1 presents use cases related to the SALTed design process. Use cases are commonly employed by software engineers to visualise a system architecture and to understand a system's main functionalities. A use case typically describes the interactions between an actor and a system. An actor in the use case represents the role of a user. We use the same approach to describe the various activities involved in the SALTed design process and the interactions of the users with the SALT framework. For each use cases, we identify the primary actor and describe its actions performed in the use case description. Note that the naming of the actor only reflects a user's role with respect to the SALT framework from a software engineering point of view.

Table 1. Use cases related to a SALTed design process

Use case	Description	Primary actor
SALT template modification	Modification of the formatting structure used to store SALT references (privacy and accountability related information) into a given repository	SALT authority
Creation of a SALT framework reference	Creation and storage (within a repository) of a standard SALT framework reference	Standards body
Extension of a SALT framework reference	Extension and storage (within a repository) of a standard SALT framework reference	Standards body
Creation of a SALT framework project reference (SFPR)	Creation and storage (within a repository) of a SALT framework project reference (references specific to a given project)	Project stakeholder
Surveillance system design	Design of an entire surveillance system	System designer
Providing technological components capabilities	Delivery of technical components capabilities	Technology provider

Note that we envision that at the beginning, the experts who initialise the SALT framework will assume the role of SALT authority. The Standards body could also be called "standards committee", which refers to persons with sufficient knowledge to create a SALT framework reference. They can be considered as experts in social-contextual, ethical, legal and technical concerns.

Based on the use cases specification, we use an activity diagram to show the interactions between the actors and their actions within the SALTed design process. The activity diagram in Fig. 3 depicts all actors and how their roles are

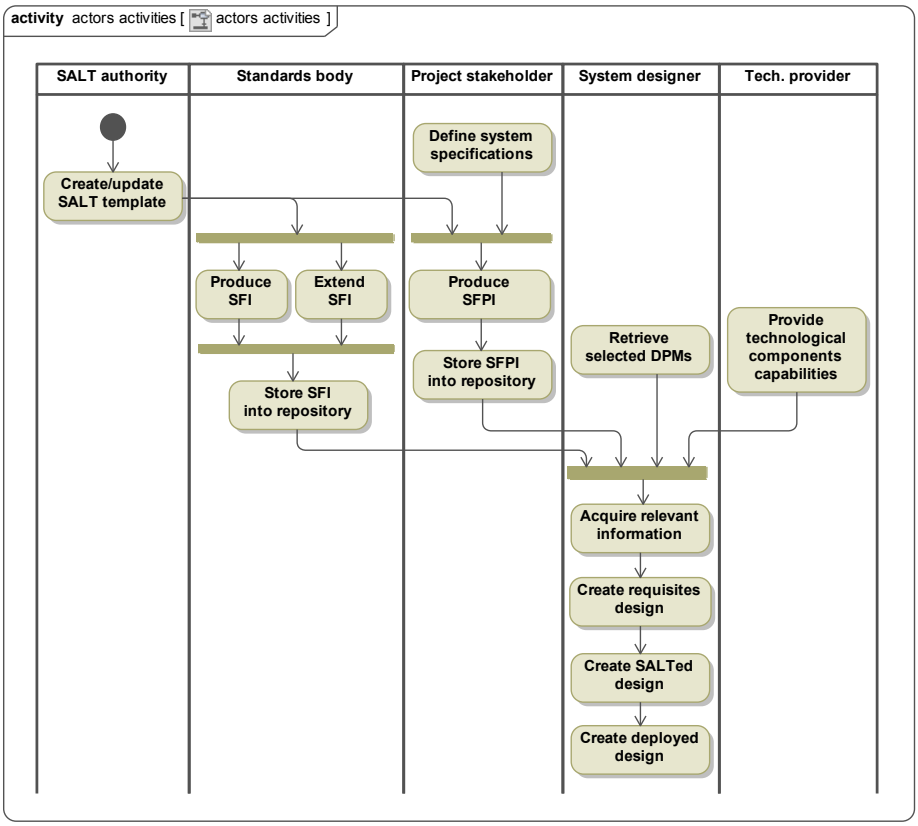

Fig. 3. Activity diagram for a SALTed design process

related. In general, the following activities can be involved in a SALTed design process:

- First, a SALT template is created if it does not yet exist. If the SALT template is already available, it is necessary to check whether the template needs to be updated according to the new information that is going to be included in the repository. Therefore, the template will be updated when needed.
- Second, information is collected according to the fields specified in the template. As the template is a part of the SALT knowledge repository, the repository is populated with related knowledge by various actors. For example, the standard body can either create or extend existing knowledge, update and store this information, i.e. SALTed Framework Instances (SFIs), into the repository. The project stakeholder can specify system requirements (considered as high level system specifications), create and store this information, i.e. SALT framework project instances (SFPIs), into the repository. In

addition, the technology provider can provide information on their component capabilities.
- Third, the system designer acquires the relevant information produced in the second step. Besides, the system designer can also include domain specific privacy knowledge represented as Domain Privacy Models (DPMs) in the SALT framework. A system design is created by the system designer. At first, a required system design without the SALT information is generated. Taking into account SALT information, then the system designer converts the design to a SALT compliant design. A final deployed system design is produced according to component capabilities and deployment scenarios. Note that the system design can be an iterative process.

6 Conclusion

We have presented a multidisciplinary approach to take into account privacy in the design of video surveillance systems. The SALT framework is a set of concepts, overarching principles, and knowledge relative to the social-contextual, ethical, legal, and technical aspects of surveillance, as well as concepts related to privacy-by-design and accountability-by-design. With the associated processes, the SALT framework serves as a decision support to assist system designer and other stakeholders in coping with complex privacy requirements in a systematic and methodological way.

The work performed so far has concentrated on the design of an architecture for the SALT Framework and reining the vision of the project. The forthcoming challenges include giving an adequate representation of social knowledge in a computer-readable format, as well as the development of tools to access, update and use the stored knowledge. The project aims at testing the methodology in two different settings: the design of a video surveillance system and a biometric system.

The approach presented here stems from the ongoing PrivAcy pReserving Infrastructure for Surveillance (PARIS) project [2]. The project gives us a unique opportunity to work together with researchers and engineers from different disciplines and backgrounds to address privacy in surveillance in a coherent way. Our interaction underlines contrasting approaches to privacy, even among consortium partners. This convinces us that a multidisciplinary approach, although sometimes difficult, is fruitful to systematically address privacy and cross-boundary issues.

Acknowledgement This work was partially funded by the European Commission though the project PrivAcy pReserving Infrastructure for Surveillance (PARIS) with contract FP7-SEC-2012-1-312504. We thank all reviewers for their invaluable and detailed comments.

References

1. Increasing Resilience in Surveillance Societies (IRISS). `http://irissproject.eu`

2. PrivAcy pReserving Infrastructure for Surveillance (PARIS). http://www.paris-project.org
3. Surveillance, Privacy and Ethics (SAPIENT). http://www.sapientproject.eu
4. Surveillance, Privacy and Security (SurPRISE). http://surprise-project.eu
5. The VideoSense Network of Excellence. http://www.videosense.eu
6. Article 29 Data Protection Working Party: Opinion 3/2010 on the principle of accountability (2010)
7. Ashley, P., Hada, S., Karjoth, G., Powers, C., Schunter, M.: Enterprise Privacy Authorization Language (EPAL). Tech. rep., IBM Research (2003)
8. Butin, D., Chicote, M., Le Métayer, D.: Log Design for Accountability. In: 2013 IEEE Security & Privacy Workshop on Data Usage Management. pp. 1–7. IEEE Computer Society (2013)
9. Butin, D., Chicote, M., Le Métayer, D.: Strong Accountability: Beyond Vague Promises. In: Gutwirth, S., Leenes, R., De Hert, P. (eds.) Reloading Data Protection, pp. 343–369. Springer (2014)
10. Cavallaro, A.: Privacy in Video Surveillance. Signal Processing Magazine, IEEE 24(2), 168–166 (2007)
11. Cederquist, J., Corin, R., Dekker, M., Etalle, S., den Hartog, J.: An Audit Logic for Accountability. In: Sahai, A., Winsborough, W. (eds.) Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks. pp. 34–43. IEEE Computer Society Press (2005)
12. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (2012)
13. Finn, R.L., Wright, D., Friedewald, M.: Seven Types of Privacy. In: Gutwirth, S., Leenes, R., Hert, P.D., Poullet, Y. (eds.) European Data Protection: Coming of Age, pp. 3–32. Springer (2013)
14. Gayrel, C., Trussart, N., Coudert, F., Maña, A., Jaime, F., Hidalgo, C., Casado, F., Ma, Z., Strobl, B., Hidalgo, V.M., Bossuet, M., Le Métayer, D., Kung, A., Jouvray, C.: PARIS Deliverable 2.1: Contexts and Concepts for SALT Frameworks. http://www.paris-project.org/images/Paris/pdfFiles/PARIS_D2.1_v1.0.pdf
15. Gill, M., Spriggs, A.: Home Office Research Study 292: Assessing the impact of CCTV. https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf (2005)
16. Russo, S.: Digital Video Surveillance: enhancing physical security with analytic capabilities. http://www-935.ibm.com/services/us/gts/pdf/sp_wp_digital-video-surveillance.pdf (2008)
17. Senior, A.W. (ed.): Protecting Privacy in Video Surveillance. Springer (2009)
18. Senior, A.W., Pankanti, S., Hampapur, A., Brown, L.M.G., li Tian, Y., Ekin, A., Connell, J.H., Shu, C.F., Lu, M.: Enabling Video Privacy through Computer Vision. IEEE Security & Privacy 3(3), 50–57 (2005)
19. Studer, R., Benjamins, V.R., Fensel, D.: Knowledge Engineering: Principles and methods. Data Knowl. Eng. 25(1-2), 161–197 (1998)
20. Trabelsi, S., Njeh, A., Bussard, L., Neven, G.: PPL Engine: A Symmetric Architecture for Privacy Policy Handling. W3C Workshop on Privacy and data usage control (2010)
21. Webster, C.W.R., Töpfer, E., Klauser, F.R., Raab, C.D. (eds.): Video Surveillance: Practices and Policies in Europe. IOS Press (2012)
22. Wright, D., Gellert, R., Gutwirth, S., Friedewald, M.: Minimizing Technology Risks with PIAs, Precaution, and Participation. Technology and Society Magazine, IEEE 30(4), 47–54 (2011)